LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for centralized processing of hardware tokens for PKI solutions comprising:

receiving a commercially available token at a secure processing facility;

installing an operating system on the token at the secure processing facility;

creating a unique key encipherment certificate that comprises a public key for the token;

writing the unique key encipherment certificate on to the token at the secure processing facility;

writing a Root Certificate Authority certificate onto the token at the secure processing facility;

writing a unique private key onto the token at the secure processing facility, the unique private key being the matching key for the unique key encipherment certificate; and

loading a software package onto the token at the secure processing facility, the software package capable of cryptologically validating future keys and certificates, decrypting the keys and certificates, and installing the keys and certificates in the token.

2. (Currently Amended) The method according to claim 1, further comprising wiping the contents of the token at the secure processing facility after the receiving.

3. (Original) The method according to claim 1, further comprising validating the operating system before the installing.

4. (Original) The method according to claim 1, further comprising writing the unique key encipherment certificate to a Read Only Memory (ROM) on the token.

5. (Currently Amended) The method according to claim 1, further comprising:

receiving the commercially available token at a workstation;

installing the token in the workstation; and

~~performing the installing, first second and third writing, and the loading remotely from the secure processing facility to the token at the workstation~~

receiving, at the workstation, data encrypted by the token's unique key encipherment certificate that can be decrypted only by the token's unique private key.

6. (Currently Amended) The method according to claim 1, further comprising performing the installing, first second and third writing, and the loading using a ~~DataCard 9000~~smartcard machine.

7. (Canceled)

8. (Original) The method according to claim 1, further comprising maintaining a copy of the public key of the token at the secure processing facility.

9. (Original) The method according to claim 1, further comprising sending at least one of a new key and a new certificate to the token remotely by the secure processing facility using a secure communication between the secure processing facility and the token, the token being attached to a remote processing device.

10. (Original) The method according to claim 9, further comprising encrypting the at least one of the new key and the new certificate using the public key of the token.

11. (Original) The method according to claim 10, further comprising validating that the at least one of the new key and the new certificate was sent from the secure processing facility using the Root Certificate Authority certificate on the token.

12. (Original) The method according to claim 1, further comprising receiving a request for the token from a user before the installing.

13. (Original) The method according to claim 12, wherein the unique key encipherment certificate comprises an identification of the user.

14. (Original) The method according to clam 13, further comprising storing a mapping of the user identification, the unique key encipherment certificate, and a serial number of the token in a database at the secure processing facility.

15. (Original) A system for centralized processing of hardware tokens for PKI solutions comprising:

a token;

a token initialization machine, the token being connectable to the token initialization machine;

a secure processing facility; and

a Root Certificate Authority, the Root Certificate Authority signing certificates of the secure processing facility, the secure processing facility receiving the token and using the token initialization machine to install an operating system on the token, write a unique key encipherment certificate onto the token, write a certificate of the Root Certificate Authority onto the token, write a unique private key onto the token, and load a software package onto the token where the software package is capable of cryptologically validating future keys and certificates, decrypting the keys and certificates, and installing the keys and certificates in the token.

16. (Original) The system according to claim 15, further comprising a crypto accelerator, the crypto accelerator being used by the secure processing facility to create the unique key

encipherment certificate and the unique private key, the unique key encipherment certificate comprising a public key for the token.

17. (Original) The system according to claim 15, wherein the token comprises a smartcard.

18. (Currently Amended) The system according to claim 15, wherein the token initialization machine comprises a ~~DataCard 9000~~smartcard machine.

19. (Original) The system according to claim 15, wherein the secure processing center comprises a Certificate Authority.

20. (Canceled)

21. (Original) The system according to claim 15, wherein the token comprises a commercially available token.

22. (Original) The system according to claim 15, wherein the secure processing facility includes:

a database, the database storing a mapping of a user identification, the unique key encipherment certificate, and a serial number of the token; and

a storage device, the storage device storing all public keys on the token.

23. (Original) An apparatus comprising a storage medium containing instructions stored therein, the instructions when executed causing a computing device to perform:

receiving a commercially available token;

installing an operating system on the token;

writing the unique key encipherment certificate onto the token;

writing a Root Certificate Authority certificate onto the token;

writing a unique private key onto the token, the unique private key being the matching key for the unique key encipherment certificate; and

loading a software package onto the token, the software package capable of cryptologically validating future keys an certificates, decrypting the keys and certificates, and installing the keys and certificates in the token.

24. (Original) The apparatus according to claim 23, the computing device further performing creating a unique key encipherment certificate that comprises a public key for the token.